VM-SERIES FOR KVM

KVM (Kernel-based Virtual Machine) is a leading open source hypervisor that service providers and enterprises alike are using to build and deploy cloud computing environments. Linux® KVM, in conjunction with OpenStack®, represents a complete open source–based solution that allows you to compound the cost reduction benefits derived through cloud computing efficiencies with the benefits of an open source solution.

VM-Series of KVM Use Cases

Palo Alto Networks® VM-Series firewalls give your organization the flexibility to deploy next-generation security and advanced threat prevention across your KVM-based private, public and hybrid cloud computing environments.

- Identify and control traffic flowing into and within your KVM-based cloud computing environment; limit application access based on users; block known and unknown threats.
- Automate security policy updates so they keep pace with changes to your private, public and hybrid clouds.
- Manage both virtual and physical form factor appliances using Panorama and automate security with a rich set of restful APIs.

Organizations are expanding their virtualization and cloud initiatives in a variety of ways with security remaining top of mind. Increased use dictates an effort for more streamlined security workflows and an eye toward cloud-centric architectures that are scalable and resilient.

- More workloads are now virtualized on premise (private cloud) than ever before, and the use of the public cloud is increasing dramatically, leading to multi-vendor (private and public) environments, along with increased demands on capacities. Additional initiative examples include security deployed as an NFV component as a more cost-effective alternative to secure branch offices and data center/private cloud workloads as well as an uptick in virtualization to address demands for [more] complete tenant isolation in multi-tenancy environments.
- Cloud security automation workflows have streamlined deployments, but they can still be complex and involve many carefully orchestrated steps.
- Security, traditionally viewed as a bottleneck that slows deployment, must more readily support the move toward cloud-centric architectures.
The VM-Series for KVM addresses these key challenges with the same Next-Generation Firewall and advanced threat prevention features that are available on our physical form-factor appliances. All traffic is natively analyzed in a single pass to determine the application identity, the content within, and who the user is. The application, content, and user identity are then used as integral components of your security policy, allowing you to tightly control access to your cloud computing resources and isolate your mission critical applications, protecting them from known and unknown threats.

The Palo Alto Networks VM-Series for KVM allows you to protect your data that resides in OpenStack and KVM based virtualized environments from cyberthreats with our next-generation firewall security and advanced threat prevention features. Panorama™ network security management, combined with native automation features, allows you to streamline policy management in a manner that minimizes the policy time-gap that may occur as virtual machines are added, removed or moved.

**Virtualized Next-Generation Security at High-Performance and Scale**

The VM-Series virtualized Next-Generation Firewall has been optimized and expanded to deliver App-ID™ enabled throughput that ranges from 200Mbps to 16Gbps across five models, both of which are industry-leading metrics. The VM-Series models include:

- The VM-50 is optimized to consume minimal resources and support CPU oversubscription, yet deliver up to 200Mbps of App-ID enabled firewall performance for customer scenarios that range from virtual branch office/customer premise equipment (CPE) to high-density, multi-tenancy environments.
- The VM-100 and VM-300 have been optimized to deliver performance at 2Gbps and 4Gbps of App-ID enabled firewall performance for hybrid cloud, segmentation, and internet gateway use cases.
- The VM-500 and VM-700 deliver an industry-leading 8Gbps to 16Gbps of App-ID enabled firewall performance respectively and can be deployed as NFV security components in fully virtualized data center and service provider environments.

Intel® Data Plane Development Kit (DPDK) has been integrated into the VM-Series for KVM for enhanced packet processing performance on x86 infrastructure. Network I/O options, such as PCI passthrough and single-root I/O virtualization (SR-IOV) are supported for enhanced performance.

**Applying Next-Generation Security to Virtualized Environments**

The VM-Series virtualized firewall is based upon the same full-stack traffic classification engine that can be found in our physical form-factor firewalls. The VM-Series natively classifies all traffic, inclusive of applications, threats and content, then ties that traffic to the user. The application, content, and user – the elements that run your business – are then used as the basis of your virtualized security policies, resulting in an improved security posture and a reduction in incident response time.

**Isolate Mission-Critical Applications and Data Using Zero Trust Principles**

Security best-practices dictate that your mission-critical applications and data should be isolated in secure segments using Zero Trust (never trust, always verify) principles at each segmentation point. The VM-Series can be deployed throughout your virtualized environment, residing as a gateway within your virtual network or in between the VMs running in different tiers, thereby protecting east-west traffic, by exerting control based on application and user identity.

**Block Lateral Movement of Cyberthreats**

Today’s cyberthreats will commonly compromise an individual workstation or user and then they will move across the network, looking for a target. Within your virtual network, cyberthreats will move laterally and rapidly from VM to VM, in an east-west manner, placing your mission-critical applications and data at risk. Exerting application-level control using Zero Trust principles in between VMs will reduce the threat footprint while applying policies to block both known and unknown threats.

**Automated, Transparent Deployment and Provisioning**

A rich set of APIs can be used to integrate with external orchestration and management tools, collecting information related to workload changes, which can then be used to dynamically drive policy updates via VM monitoring and Dynamic Address Groups.

- **RESTful APIs:** A flexible REST-based API allows you to integrate with third-party or custom cloud orchestration solutions. This enables the VM-Series to be deployed and configured in lockstep with virtualized workloads.
- **Virtual machine monitoring:** Security policies must be able to monitor and keep up with changes in virtualization environments, including VM attributes and the addition or removal of VMs. Virtual machine monitoring (VM monitoring) automatically polls your virtualization environments for virtual machine inventory and changes, collecting this data in the form of tags that can then be used in Dynamic Address Groups to keep policies up to date.
- **Dynamic Address Groups:** As your virtual machines change functions or move from server to server, building security policies based on static data, such as IP address, delivers limited value and can contain outdated information. Dynamic Address Groups allows you to create policies using tags [from VM monitoring] as an identifier for virtual machines instead of a static object definition. Multiple tags representing virtual machine attributes, such as IP address and operating system, can be resolved within a Dynamic Address Group, allowing you to easily apply policies to virtual machines as they are created or travel across the network without administrative intervention.
• **Bootstrapping:** In addition to XML template-based bootstrapping for KVM-based virtual environments, VM-Series firewalls in OpenStack environments support ‘Config-Drive’ for sharing meta-data. With these bootstrapping approaches, the VM-Series can be modified at deployment time, effectively delivering a customized firewall during the initial provisioning process.

**Centrally Manage Virtualized and Physical Form-Factor Firewalls**

Panorama allows you to manage your VM-Series deployments along with your physical security appliances, thereby ensuring policy consistency and cohesiveness. Rich centralized logging and reporting capabilities provide visibility into virtualized applications, users and content.

**VM-Series for KVM Use Case: Perimeter Gateway**

For enterprises embarking down a build-your-own cloud computing environment, the VM-Series for KVM allows you to apply all of the Palo Alto Networks Next-Generation Firewall and advanced threat prevention features to the traffic traversing your cloud computing perimeter.

In this use case, the VM-Series for KVM can be deployed as your gateway firewall, and you can enable the applications you want and inspect them for known and unknown threats, regardless of port. Access to the virtualized workloads is controlled based on user identity, adding yet another level of protection. As new workloads are added or changed, VM-Series automation features, APIs and an optional OpenStack plugin allow you to dynamically update security policies ensuring they keep pace with your respective cloud computing changes.

**VM-Series for KVM Use Case: Service Provider Customer Offerings**

KVM and OpenStack are commonly used by service providers to efficiently and cost-effectively scale their cloud computing service offerings for customers. The open source nature of the solution offering lends itself to highly customized and differentiated services, such as virtualized CPE(vCPE) deployments, SD-WAN solutions and, for large enterprise customers, high-capacity virtualized network-based security services. When combined with the Next-Generation Firewall and automation features in the VM-Series, service providers can build highly profitable cloud computing service offerings.

**Performance and Capacities Summary**

The security performance table listed below is tested under controlled lab conditions with PAN-OS® 8.0. In virtualized and cloud environments, many factors, such as type of CPU, hypervisor version, numbers of cores assigned, memory and network I/O options, can impact your performance. We recommend additional testing within your environment to ensure your performance and capacity requirements are met.

<table>
<thead>
<tr>
<th>Performance and Capacities</th>
<th>VM-50 (0.4 core)</th>
<th>VM-100/VM200 (2 Cores)</th>
<th>VM-300/VM-1000-HV (4 Cores)</th>
<th>VM-500 (8 Cores)</th>
<th>VM-700 (16 cores)</th>
</tr>
</thead>
<tbody>
<tr>
<td>With Single-Root I/O Virtualization (SR-IOV)/PCI Passthrough of I/O Enabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall throughput (App-ID enabled)</td>
<td>200 Mbps</td>
<td>2 Gbps</td>
<td>4 Gbps</td>
<td>8 Gbps</td>
<td>16 Gbps</td>
</tr>
<tr>
<td>Threat prevention throughput</td>
<td>100 Mbps</td>
<td>1 Gbps</td>
<td>2 Gbps</td>
<td>4 Gbps</td>
<td>8 Gbps</td>
</tr>
<tr>
<td>IPsec VPN throughput*</td>
<td>In process</td>
<td>In process</td>
<td>In process</td>
<td>In process</td>
<td>In process</td>
</tr>
<tr>
<td>With open virtual switch OVS-DPDK</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall throughput (App-ID enabled)</td>
<td>100 Mbps</td>
<td>1 Gbps</td>
<td>2 Gbps</td>
<td>4 Gbps</td>
<td>8 Gbps</td>
</tr>
<tr>
<td>Threat prevention throughput</td>
<td>50 Mbps</td>
<td>500 Mbps</td>
<td>1 Gbps</td>
<td>2 Gbps</td>
<td>4 Gbps</td>
</tr>
<tr>
<td>IPsec VPN throughput*</td>
<td>In process</td>
<td>In process</td>
<td>In process</td>
<td>In process</td>
<td>In process</td>
</tr>
</tbody>
</table>

**Capacities**

<table>
<thead>
<tr>
<th></th>
<th>VM-50 (0.4 core)</th>
<th>VM-100/VM200 (2 Cores)</th>
<th>VM-300/VM-1000-HV (4 Cores)</th>
<th>VM-500 (8 Cores)</th>
<th>VM-700 (16 cores)</th>
</tr>
</thead>
<tbody>
<tr>
<td>New sessions per second</td>
<td>3,000</td>
<td>8,000</td>
<td>15,000</td>
<td>30,000</td>
<td>60,000</td>
</tr>
<tr>
<td>Max sessions</td>
<td>50,000</td>
<td>250,000</td>
<td>800,000</td>
<td>2,000,000</td>
<td>10,000,000</td>
</tr>
</tbody>
</table>

*IPsec VPN throughput data will be published upon completion of the test suite

The performance and capacities results shown above were tested under following conditions:

- Firewall and IPsec VPN throughput are measured with App-ID and User-ID features enabled.
- Threat prevention throughput is measured with App-ID, User-ID, IPS, antivirus and anti-spyware features enabled.
- Throughput is measured with 64KB HTTP transactions.
- Connections-per-second is measured with 4KB HTTP transactions.
VM-Series Specifications and Features
The tables below list all supported specifications, resource requirements and networking features on VM-Series for VMware® NSX™.

**VIRTUALIZATION SPECIFICATIONS**

<table>
<thead>
<tr>
<th>Image formats supported</th>
<th>QCOW2</th>
</tr>
</thead>
</table>
| Hypervisors supported   | KVM on CentOS  
                          | Red Hat Enterprise Linux® (RHEL)  
                          | KVM on Ubuntu® |
| Network I/O options     | • Virtio  
                          | • Paravirtual drivers (Intel e1000)  
                          | • PCI pass-through  
                          | • Single-root I/O Virtualization (SR-IOV) |
| Bootstrap support       | • XML template based bootstrap in KVM environments  
                          | • 'Config-Drive' with nova boot in OpenStack |
| OpenStack distributions supported | • Mirantis OpenStack  
                                      | • Red Hat OpenStack |

**SYSTEM REQUIREMENTS**

<table>
<thead>
<tr>
<th></th>
<th>VM-50 (0.4 Core)</th>
<th>VM-100/VM-200 (2 Cores)</th>
<th>VM-300/VM-1000-HV (4 Cores)</th>
<th>VM-500 (8 Cores)</th>
<th>VM-700 (16 Cores)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU configurations supported</td>
<td>2²</td>
<td>2</td>
<td>2.4</td>
<td>2.4 and 8</td>
<td>2.4,8 and 16</td>
</tr>
<tr>
<td>Memory (minimum)</td>
<td>4.5GB</td>
<td>6.5GB</td>
<td>9GB</td>
<td>16GB</td>
<td>56GB</td>
</tr>
<tr>
<td>Disk-drive capacity (min/max)</td>
<td>32GB/2 TB</td>
<td>60GB/2TB</td>
<td>60GB/2TB</td>
<td>60GB/2TB</td>
<td>60GB/2TB</td>
</tr>
</tbody>
</table>

1. CPU oversubscription is supported with up to five instances running on a 2 CPU core configuration  
2. 60GB drive capacity is needed on initial boot. VM-series instance will use 32GB after license activation

**Networking Features**

**Interface Modes:**

- L2, L3, Tap and virtual wire (transparent mode)

**VLANs**

- 802.1q VLAN tags per device/per interface: 4,094/4,094
- Max interfaces: 4,096 (VM-500/VM-700)  
  2048 (VM-100/VM-300)  
  512 (VM-50)

**Routing**

- **Modes:** OSPF, RIP, BGP, Static  
  Policy-based forwarding  
  Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3

**Network Address Translation (NAT)**

- NAT modes (IPv4): Static IP, Dynamic IP, Dynamic IP and Port (port address translation)  
  NAT64  
  **Additional NAT features:** Dynamic IP reservation, Dynamic IP and Port oversubscription

**High Availability**

- **Modes:** Active/Passive with session synchronization  
  **Failure detection:** Path monitoring, Interface monitoring

**IPv6**

- L2, L3, tap, virtual wire (transparent mode)  
  **Features:** App-ID, User-ID, Content-ID, WildFire and SSL decryption

**Summary**

The VM-Series for KVM allows service provider and enterprise customers alike to protect their cloud computing environments with full next-generation firewall and threat prevention services. Traffic flowing into your KVM-based cloud is identified based on the application, then inspected for known and unknown cyberthreats. Automation features and centralized management with Panorama ensure that security policy can keep pace with any contextual changes in your cloud computing environment.

To view additional information on the VM-Series security features and associated capacities, please visit www.paloaltonetworks.com/products.